Incident Response threat summary for July - September 2021

WATCH OUT FOR SPAM ATTACKS, AS BUSINESS EMAIL COMPROMISE IS ON THE RISE

THE TAKEAWAY

Ransomware was once again the top threat this quarter that Cisco Talos Incident Response (CTIR) saw in their engagements in Q3 2021. This quarter featured a wider variety of emerging variants compared to previous quarters, where ransomware threats like Ryuk dominated the threat landscape. The well-known ransomware REvil and newcomer Vice Society were the only ransomware threats seen in more than on engagement this quarter. While ransomware variants are still a concern, this highlights a greater democratization of emerging variants.

TOP THREATS

- Ransomware was the clear top threat this quarter, comprising nearly 38 percent of all threats, which is slightly down from last quarter.
- This quarter saw the most business email compromise (BEC) incidents since we began compiling these reports in late 2019.
- We saw several new ransomware threats with families like the aforementioned Vice Society, Hive, Karma, Grief, CryptBD and Thanos appearing for the first time.
- REvil attackers exploited Kaseya VSA using CVE-2021-30116 and their managed service providers, the latest in a string of supply chain attacks this year.
- CTIR engaged in two incidents involving the information-stealer Redline, a relatively new threat that emerged in 2020 and will usually spread via malicious advertisements and phishing emails.

OTHER LESSONS

- We saw a rise in the use of remote access software, such as AnyDesk and TeamViewer, and command line utilities such as PsExec.
- In engagements that have yet to close out, we have also continued to see this trend of using remote access tooling, including software such as SplashTop and Atera, that we typically do not observe in engagements.
- Local government agencies were the most-targeted vertical this quarter, surpassing health care. Other industries targeted include hospitality, local government, financial services, IT, entertainment and retail.
- We are also currently engaging in several suspected pre-ransomware incidents where ransomware was never deployed, but attackers still deployed red team frameworks such as Cobalt Strike and Sharphound.

HOW ARE OUR CUSTOMERS PROTECTED?

- Using multi-factor authentication, such as Cisco Duo, will help prevent adversaries from accessing users' accounts and spreading malware deeper into networks. CTIR frequently observes ransomware incidents that could have been prevented if MFA had been enabled on critical services.
- Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of any BEC campaigns. You can try Secure Email for free here.
- Should an infection occur, having a CTIR retainer gives customers peace of mind that they will have help as soon as possible from our experts.
- Cisco Secure Endpoint is ideally suited to prevent the execution of ransomware and other malware families. Try Secure Endpoint for free here.